Help! My Mobile Device is Spying on Me

Delivered by Murray Goldschmidt, Chief Operating Officer

AusCERT 2012 Conference, 17 May 2012

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney
Level 8, 66 King Street
Sydney NSW 2000
Australia

Melbourne
Level 10, 401 Docklands Drv
Docklands VIC 3008
Australia

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

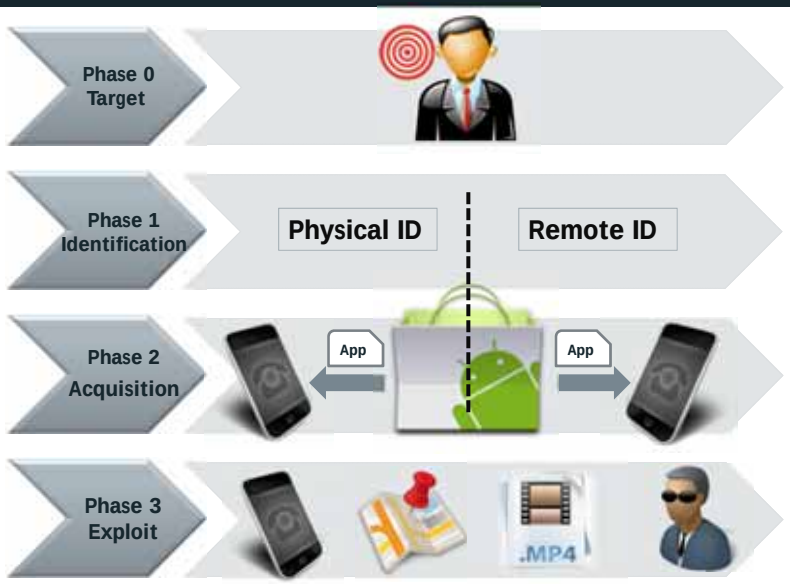
info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

Agenda

Our "Targeted Voice Recorder" research addresses

- Relevance - Extent of exposure
- Simplicity - Anatomy of the attack
- Protection - Mitigating controls

High Level Process Flow



Mobile Device Platforms

Android - Path of Least Resistance

- Volume of devices and growth
- Market fragmentation
- Lag for software updates
- Open platform
- Vetting controls

Proof of Concept - Overview

- Objective: Obtain a voice recording of the user using the device (not phone call)

Requires:

- Knowledge of their mobile device platform
- Physical or remote acquisition techniques
- A mobile app that can trigger at a specific location, act as a recorder and post recorded files
- An app that is in the market place (ideally)
- An app that can be remote controlled (ideally)

Simple but Efficient




Simple but Effective (Devastating)

Voice recorder - > Targeted Individual

~ 600 LOC

- **Corporate Espionage**
- **Insider Trading**
- **Financial Gain**
- **Political Gain**
- **Competitive Advantage**

~ $few hundred

Proof of Concept - Application

Functions

- ~600 Lines of Code
- Polls a specific server for instructions (where to trigger, radius, duration)
- Triggers on GPS co-ordinates (or derived location from GSM Network, Wireless etc)
- Records for 30 seconds. Continuous looping for demo.

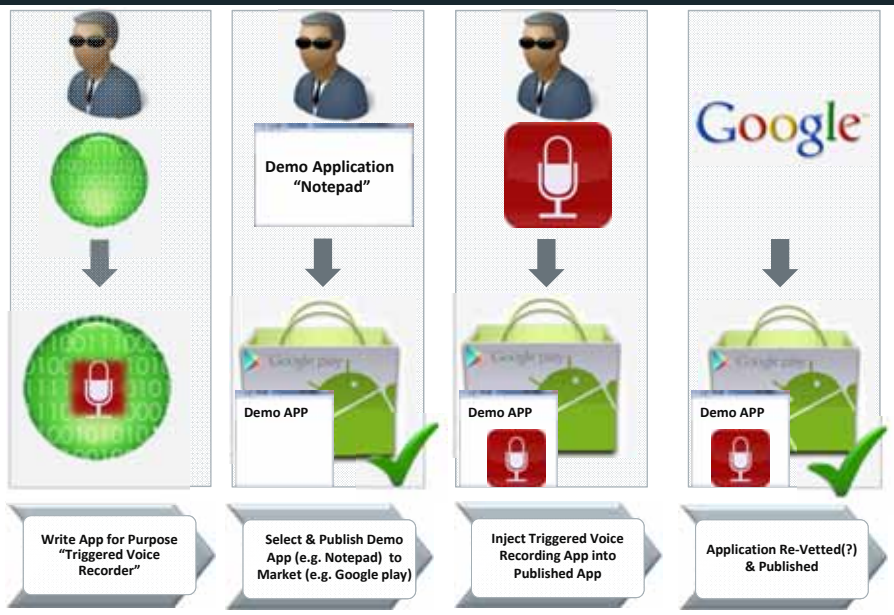
Permissions Required

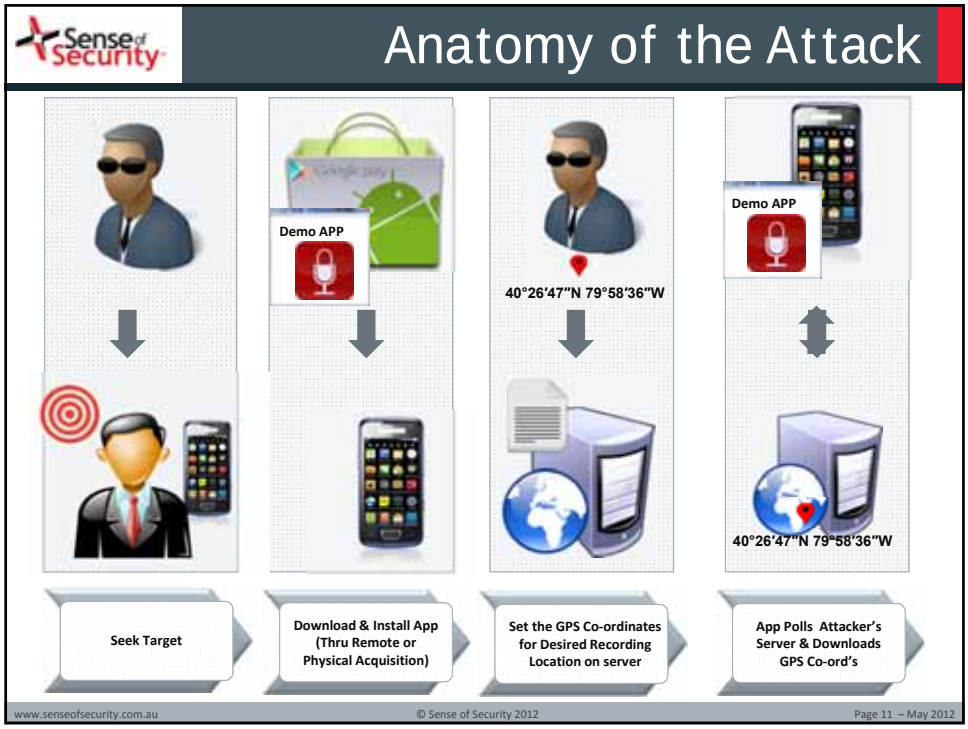
- access your location (GPS)
- your personal information (contact info)
- network communications (make outbound connections)
- storage (store file)
- hardware controls (record audio)

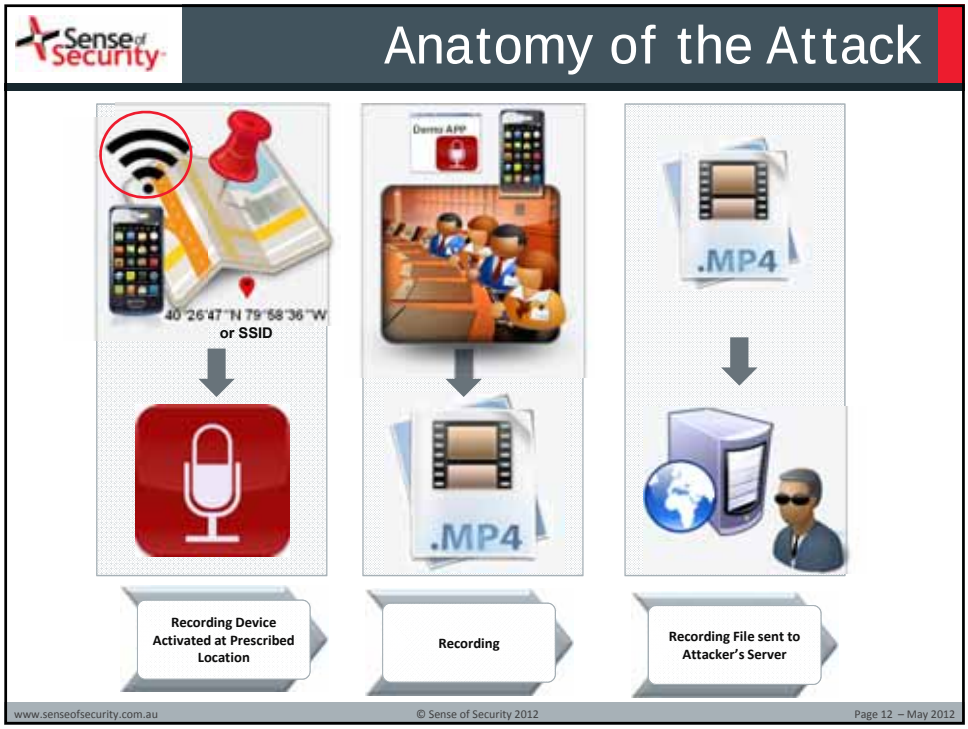
Visibility

- None – will operate in the background and not alert the owner it is triggered (although PoC app presents logging information on the screen for demo purposes, and vibrates to indicate recording!)

Anatomy of the Attack




Anatomy of the Attack
Demo APP
40°26'47"N 79°58'36"W
Demo APP
40°26'47"N 79°58'36"W
Seek Target
Download & Install App (Thru Remote or Physical Acquisition)
Set the GPS Co-ordinates for Desired Recording Location on server
App Polls Attacker's Server & Downloads GPS Co-ord's
www.senseofsecurity.com.au
© Sense of Security 2012
Page 11 – May 2012


Anatomy of the Attack
40°26'47"N 79°58'36"W
or SSID
Demo APP
.MP4
.MP4
Recording Device Activated at Prescribed Location
Recording
Recording File sent to Attacker's Server
www.senseofsecurity.com.au
© Sense of Security 2012
Page 12 – May 2012

Demo

Physical Identification

Lobby

Elevator

Exec Desk

Coffee Shop

Physical Acquisition

No Password

No pin/password controls by default;
Not complex by default

Remote Identification & Acquisition

Email Trailer — Sent from my HTC Velocity 4G on the Next G network

User Agent Info

Gmail Compromise

Drive by Download

Spear Phishing

Broader Implications

- Access to Personal or Corporate Email
- Access to SMS
- Access to Images
- Access to Network (personal, wireless, corporate, VPN)
- Access to Corporate Apps & Data
- Send SMS to Premium Rated Services "Toll Fraud"

Controls and Mitigations

Controls that will assist in addressing this issue

- Whitelist specific applications (or blacklist 2nd pref)
- Educate users on best practices regarding mobile devices
- Strong alphanumeric passcode; smudge protection
- Restrict default apps and resources such as browser, camera, YouTube, and Google Play

Controls and Mitigations

Other MDM controls that should be considered … but won't all address this issue

Bring corporate and employee-owned phones under centralised IT management

Connect mobile devices securely to enterprise resources including email, Wi-Fi and VPN

Enforce security policies to protect corporate data

Configure device security such as encryption of data-at-rest and passcodes

Enforce secure bring your own device (BYOD) policies if you allow staff to use their devices inside the network

Controls and Mitigations

Keep highly confidential data off mobile devices

No removable media such as SD cards allowed in corporate mobile devices

Block attachment execution or downloading to the SD card

Detect rooted devices and remote wipe when found

Internal segregation controls on what access mobile devices have inside the network

Controls and Mitigations

- Expedite handling to secure lost, stolen or retired smartphones through full and selective wipe
- Rogue app protection as well as inventories of installed apps
- Ensure anti malware/anti virus is up to date
- Define and enforce allowed device types, OS, and patch levels

Mobile Device Platforms

These attacks are valid across the other major platforms.

SOS Research

Special note of thanks to the dedicated, motivated and highly talented team at SOS.

This presentation is the culmination of a research program delivered through effective collaboration, teamwork and perseverance to push the envelope on the cutting edge.

Conclusion

- Extreme exposure
- Severe implications for privacy of the individual
- Severe implications for confidentiality of information for business/government
- The fact that every person has/will have a mobile device means that every person is a walking/moving/sitting voice/video recorder that can be exploited
- Remote control capability to spy extends the scope and risk
- MDM controls are good for general security – but not all will address this issue
- Requires user education; however curiosity of users and inclination to trust will result in continued exposure

Questions?

Thank you

Recognised as Australia's fastest growing information security and risk management consulting firm through the Deloitte Technology Fast 50 & BRW Fast 100 programs

This presentation will be published at
http://www.senseofsecurity.com.au/research/presentations

Whitepaper will be published at
http://www.senseofsecurity.com.au/research/it-security-articles

Attribution – icons from iconfinder.com

Sydney, Melbourne
T: 1300 922 923
info@senseofsecurity.com.au
www.senseofsecurity.com.au